SOLUTION OVERVIEW

F5 Adds Enhanced Security to AWS-Hosted Public Sector Apps

Protect your government cloud-based applications from advanced threats.

OWASP TOP 10 WEB APPLICATION SECURITY RISKS[1]

- Broken access control
- Cryptographic failures
- Injection
- Insecure design
- Security misconfiguration
- Vulnerable and outdated components
- Identification and authentication failures
- Software and data integrity failures
- Security logging and monitoring failures
- Server-side request forgery

Application modernization is building momentum in the public sector and agencies are more reliant on them to achieve IT goals. While adding productivity, more apps mean more potential vulnerabilities that can be exploited. A recent study discovered that 52% of all data breaches were the result of attacks on web apps.[2]

The recent Cybersecurity Executive Order from the White House shows a great example of a clear escalation from government on what is required to keep up with evolving threats, especially mitigating threats against applications.

If you're delivering applications via Amazon Web Services (AWS), a variety of native and purpose-built security tools can help thwart attacks and keep your data and constituents safe.

Leveraging Amazon CloudFront to Deliver Your App

Amazon CloudFront is a content delivery network (CDN) with low latency and high transfer speeds. Leveraging Amazon's 310+ Points of Presence, you benefit from a data center and network architecture that is designed to meet the requirements of the most security sensitive organizations. A strong security strategy relies on choosing the right tools at the outset. AWS Shield Standard is built into Amazon CloudFront and provides DDoS mitigation against layer 3 and layer 4 attacks. In addition to built-in DDoS protection, CloudFront is compliant with multiple programs. **Click here** for more information on AWS compliance programs.

Amazon CloudFront is integrated with AWS origin-based services, such as Amazon Simple Storage Service (Amazon S3), Elastic Load Balancing (ELB), Amazon Elastic Compute Cloud (Amazon EC2), Amazon API Gateway, and AWS Media Services, and also supports third-party origins (on premises, hosted environment, third-party cloud provider). Amazon CloudFront can help you accelerate and protect both dynamic and static content while reducing the load on your origin service.

Starting in the AWS Management Console, you can configure your origin and begin testing your Amazon CloudFront distribution in as little as 15 minutes.

Once you're set up, you can integrate additional layers of protection with other available services.

HOW F5 THREAT STACK WORKS WITH YOUR AWS ASSETS

F5 Threat Stack adds another layer of protection by analyzing all of your AWS assets to identify vulnerabilities in the infrastructure. Threat Stack proactively checks for security issues within your AWS environment and the native constructs that you built.

With Threat Stack, you can identify patterns of risky behavior, increase your breach detection, and reduce your time to respond.

Deploy AWS WAF on Amazon CloudFront to Protect against OWASP Top 10 Vulnerabilities

Even with reliable monitoring, given the sheer volume of attacks, it's important to set up a strong application firewall to block bad actors. AWS WAF is a web application firewall (WAF) that helps protect your web applications and application programming interfaces (APIs) against common web exploits that may affect availability, compromise security, or consume excessive resources.

AWS WAF gives you more control over traffic reaching your applications by enabling you to create security rules that mitigate against layer 7 attacks such as SQL injection or cross-site scripting (XSS).

Use F5 Managed Rules to Level up Your AWS WAF

F5 Managed Rules for AWS WAF dramatically enhances security effectiveness while reducing the operational overhead of having to write many custom rules. Rules are managed by F5's Security Threat Intelligence Team. This world-class team of researchers explores forums and third-party resources, investigates attacks, reverse engineers malware, and analyzes vulnerabilities to determine effective detection and mitigation methods that guard against web threats, DDoS attacks, and other evasive or evolving threats.

Protection provided by each of the four F5 rulesets includes:

Bot Protection Ruleset
Analyzes all incoming requests and blocks any malicious bot activities including DDoS tools, vulnerability scanners, web scrapers, and forum spam tools.

OWASP Top 10 Web Exploits Protection Ruleset
Mitigates attacks that seek to exploit vulnerabilities contained in the OWASP Top 10, including cross-site scripting (XSS) attacks, injection attacks, and many more.

API Attack Protection Ruleset
Secures against API-level attacks, as well as XML external entity attacks and server-side request forgery (SSRF); also offers support for both XML and JSON payloads and common web API frameworks.

Common Vulnerabilities and Exposures (CVE) Protection Ruleset
Defends against high-profile CVEs that can be found in popular systems such as Apache, Java, MySQL, WordPress, and many more.

USING [F5 DISTRIBUTED CLOUD BOT DEFENSE], WE ELIMINATED UNWANTED AUTOMATED BOT TRAFFIC, WHICH AT TIMES ACCOUNTED FOR 95% OF OVERALL TRAFFIC.

–Security Director, at a global airline

Enhanced Security for Advanced Attacks with F5 Distributed Cloud Bot Defense

As your application grows and sees increased visibility over time, it will be exposed to more sophisticated attacks and therefore require greater security. F5® Distributed Cloud Bot Defense is a managed security service that prevents bot attacks, which can result in large-scale fraud, inflated operational costs, and friction for your end users. By delivering continuous protection to your enterprise, the service is designed to ensure protection from the most concerning online attacks, including those on the OWASP list.

Distributed Cloud Bot Defense is an all-in-one security solution built with artificial intelligence (AI) and machine learning (ML) that leverages its global footprint and network to identify and prevent a wide range of attack tactics (bots, unauthorized online transactions, and fake users), helping organizations mitigate fraud and abuse. Distributed Cloud Bot Defense prevents fraud by securing specific endpoints on web applications that bots try to breach.

Distributed Cloud Bot Defense yields real-time insights and reporting, along with 24x7 support from the global F5 Security Operations Centers (SOC). Customers receive real-time attack details with enhanced visibility into measures taken to detect and mitigate the attack.

Distributed Cloud Bot Defense helps organizations without IT and security teams to protect their online transactions.

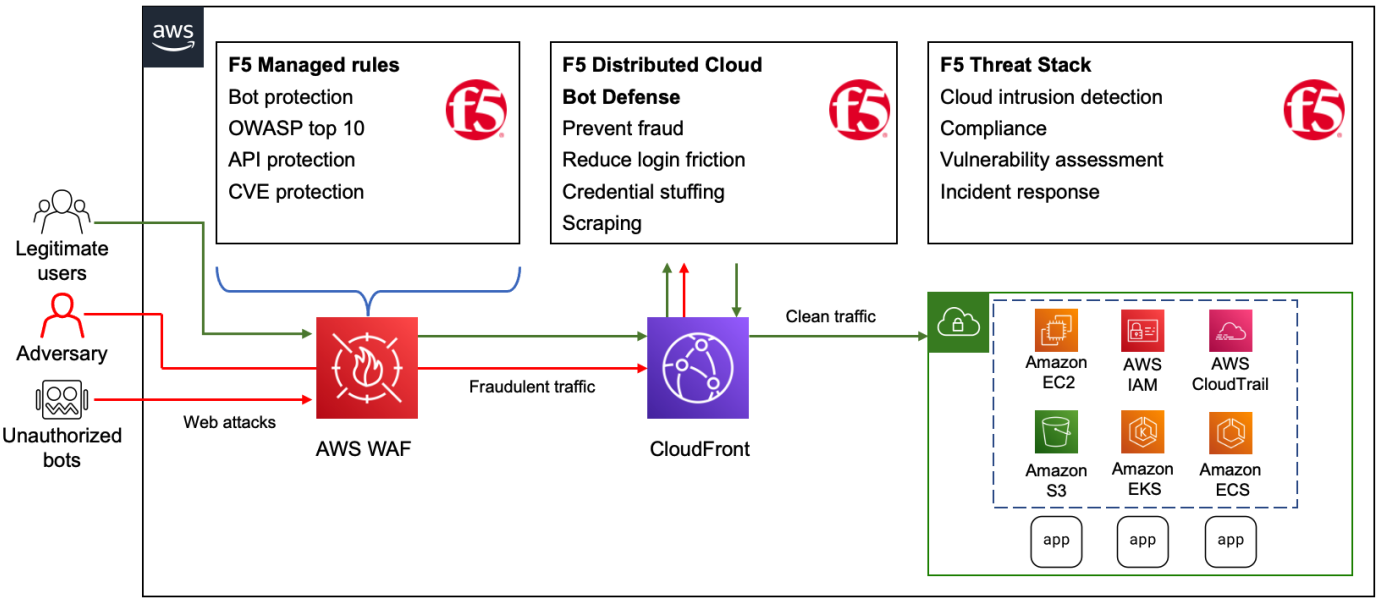

Figure 1: If you're delivering applications via Amazon Web Services (AWS), several native and purpose-built security tools can help thwart attacks to keep your data and constituents safe and maintain compliance.

How F5 Distributed Cloud Bot Defense Can Benefit Your Business

- Immediate bot mitigation and security to protect your apps.
- Effective bot detection to reduce false positives.
- Fast implementation to deliver rapid time to value.
- Full visibility of attack data for forensic analysis.
- Global threat intel is used to strengthen your policies.

Discover how Distributed Cloud Bot Defense can help protect you from fraud, breaches, and the lack of visibility into attacks.

Explore F5 Solutions on AWS and learn more about F5 Public Sector Solutions.

Appendix

[1] OWASP Top Ten, found at https://owasp.org/www-project-top-ten/

[2] Verizon Data Breach Investigations Report, 2019, found at https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis/

aws PARTNER

- Public Sector
- Marketplace Seller
- Networking Competency
- Security Software Competency